USER AGREEMENT
INDIANA CRIME INFORMATION NETWORK

"ICIN"

Please read all terms and conditions of this User Agreement ("Agreement") for the "Indiana Crime Information Network Database ("Database") before signing (please initial each page where indicated). The original signed Agreement must be maintained in the records of the Participating Agency and a copy shall be sent the Indiana Intelligence Fusion Center ("IIFC") (see also, page 12 of this User Agreement).

This Agreement applies to anyone granted access to the Database including, but not limited to, intelligence analysts, law enforcement officers, correction officers, parole officers, probation officers, and other personnel from criminal justice agencies. To use the Database, you agree to adhere to the provisions of this Agreement, which are established to ensure the appropriate use and security of the criminal intelligence information in the Database.

I. PURPOSE:

The Database is a component of the IIFC's Crime Information Sharing Project ("Project"). The purpose of the Project is to improve the collection, analysis, and sharing of crime information in the State of Indiana among law enforcement and criminal justice agencies with the intent of preventing, reducing, and solving criminal activity in conformance with the privacy and constitutional rights of subjects.

Users hereby agree that criminal intelligence information entered into or obtained from the Database will only be used for legitimate law enforcement or criminal justice purposes. A legitimate law enforcement or criminal justice purpose means that the entry and/or query of data can be directly linked to the need-to-know and right-to-know criminal intelligence information. The Database may not be accessed for the investigation of infractions that are not defined as crimes or background screening for employment purposes.

II. DEFINITIONS:

"CrimeNtel software" means the CrimeNtel Windows Version and the CrimeNtel Web Edition used for the Database.

"Criminal activity" is defined as any activity that violates state or federal law that is punishable as a misdemeanor or a felony (excluding traffic violations or other statutes that are punishable as infractions).

_____
Initials

"Criminal gang" see "Criminal organization" below.

"Criminal organization" means a group with at least three (3) members that specifically: (1) either: (A) promotes, sponsors, or assists in; or (B) participates in; or (2) requires as a condition of membership or continued membership; the commission of a felony or an act that would be a felony if committed by an adult or the offense of battery (IC 35-42-2-1).

"Criminal intelligence information" means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria.

"Criminal intelligence system or Intelligence System" means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

"Criminal justice agency" means any agency or department of any level of government which performs as its principal function the apprehension, prosecution, adjudication, incarceration, rehabilitation of criminal offenders, or location of parents with child support obligations under 42 USC § 653. The term includes the IIFC and other entities identified in IC 5-2-4-1(3)(A)-(C).

"Database" means the Indiana Crime Information Network.

"Database Administrator" means the person responsible for the administration of the Database.

"Derivative intelligence products" means an intelligence product that is generated by a User utilizing criminal intelligence information obtained from the Database.

"IIFC Security Officer" means the person whom is designated as Security Officer for the IIFC by the IIFC Executive Director.

"Interjurisdictional intelligence system" means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions.

"Need-to-know" means the necessity to obtain or receive criminal intelligence information in the performance of official responsibilities as a law enforcement or criminal justice agency or authority.

"Participating agency" means an agency of local, county, state, federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system.

"Privacy policy" is a written, published statement that articulates the policy position of the IIFC on how it handles the personal information that it gathers and uses in the normal course of business. The policy includes information relating to the processes of information collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the IIFC will adhere to those legal requirements and the IIFC policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests.

"Right-to-know" means the legal authority to obtain or receive criminal intelligence information pursuant to court order, statute, or case law.

"Reasonable suspicion or criminal predicate" is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

"User" is someone who has signed a User Agreement with the approval of his or her Participating Agency; received approval from the IIFC to directly access the Database either to enter and/or query data; and, who has been issued a logon and password by the IIFC.

"Validation of information" means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

III. MANDATORY 28 CFR Part 23 TRAINING:

28 CFR Part 23 Training is required for all Database Users and is available at https://www.ncirc.gov/28cfr/Default.aspx. The User agrees to submit a copy of the training certification received upon the satisfactory completion of the on-line training with the signed Application for ICIN access. The User also certifies awareness of the requirements of IC 5-2-4, Criminal Intelligence Information, by signing this Agreement. The User agrees to complete all IIFC required training to be granted query and/or entry rights capabilities.

IV. PRIVACY:

The IIFC's Privacy Policy is posted at www.in.gov/iifc. The User acknowledges that he or she will review and acknowledge receipt of the IIFC Privacy Policy and complete the required IIFC Privacy Policy Training module prior to submitting the Application for User access to ICIN. (see also, ICIN Application Instructions). The User acknowledges that the IIFC reserves the right to

_____
Initials

conduct inspections and audits concerning the proper use and security of the Database and compliance with the IIFC Privacy Policy requirements.

V. SECURITY:

Membership (authorized access to the Database) is offered to any member of the law enforcement and criminal justice community with a need-to-know and right-to-know criminal intelligence information who has the approval of the Participating Agency head to become a User. Technical capabilities and systems architecture protect the Database through the use of encryption, user authentication, and firewalls to prevent unauthorized access. It is critical to ensure that appropriate security safeguards are in place to protect from unauthorized use and disclosure of information in the Database. Only authorized Users who have received Database training and whose use will be monitored to ensure appropriate activity can use the Database.

The User agrees to be responsible for maintaining the required level of security to prevent unauthorized use and disclosure of information and further agrees to:

A. Safeguard Database logon and password information;
B. Refrain from sharing Database logon and password information;
C. Access the Database only at the security level granted by the IIFC;
D. Use screen locks or logoff the computer when not in the immediate area of the workstation to ensure data security is not compromised;
E. Refrain from disseminating Database criminal intelligence information to anyone who does not have the proper authorization to receive it; and,
F. Report any known or suspected security incidents or improper use of Database criminal intelligence information to the IIFC Security Officer.

The Database contains an automated tracking mechanism of system use. The IIFC, acting as the security agent for the Database, will take necessary measures to ensure that access to the Database is secure and that any unauthorized use is prevented. The IIFC reserves the right to restrict the number of personnel and the level of access and to suspend or withhold access to any individual User or Participating Agency violating this Agreement. The IIFC reserves the right to conduct inspections and audit concerning the proper use and security of the Database by Users and Participating Agencies. Appeals of decisions of the IIFC Executive Director can be made to the IIFC Executive Committee.

VI. UNAUTHORIZED USE:

The User agrees to use the Database only when he or she has a need-to-know and right-to-know criminal intelligence information. The User agrees not to collect or maintain criminal intelligence information about the political, religious or social views, association, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to the criminal conduct or activity and there is reasonable

suspicion that the subject of the information is or may be involved in criminal conduct or activity. The User agrees that the use of the Database for employment background screening is prohibited. The User agrees that the unauthorized use of the Database will be reported to the appropriate authorities and may result in administrative, civil, and criminal actions. Unacceptable uses of the Database include:

A. Illegal use – any use of the Database resources for illegal purposes or in support of such activities as defined as a violation of local, state, or federal laws;
B. Commercial use – any use for commercial purposes, products, services, advertisement, or for profit personal activity;
C. Political use – any use for political activities;
D. Intellectual property violations – any use that would constitute an infringement of copyright or trademark rights. Title to the CrimeNtel software, including ownership rights to patents, copyrights, trademarks, and trade secrets in connection with its use are the exclusive property of CI Technologies, Inc. User hereby acknowledges and agrees that he or she shall not have or accrue any title or ownership interests to the software including any ownership rights to patents, copyrights, trademarks, and trade secrets therein. User is prohibited from modifying or making copies of the CrimeNtel software;
E. Security protections – disabling security protections for any reason. The User shall report security malfunctions to the Database Administrator.

VII. TERMINATION OF USE PRIVILEGES:

If a User is found to be in noncompliance with the provisions of this Agreement the Executive Director of the IIFC will:

A. Suspend or terminate access to the Database by the User; apply administrative actions or sanctions as provided by IIFC policies; and, request that the Participating Agency initiate proceedings to discipline the User or enforce the Agreement's provisions; and,
B. Refer the matter to appropriate authorities for criminal prosecution if a violation of the Agreement constitutes a violation of any criminal laws.

Appeals of decisions of the IIFC Executive Director can be made to the IIFC Executive Committee.

VIII. CRIMINAL INTELLIGENCE INFORMATION SUBMISSION CRITERIA:

Users will be authorized either "query rights only" or authorized "query and entry rights". Users with "query rights only" may query the Database directly (automated) but may not make direct (automated) entries into the Database. Users with "query rights only" may generate submissions by: (1) contacting the IIFC, (2) submitting a Participating Agency's approved collection form to the IIFC, or (3) submitting through their Participating Agency approved User who has "query and entry rights". Users with "query and entry rights" may make direct (automated) entries into the

Database or submit entries indirectly by contacting the IIFC or by submitting a Participating Agency's approved collection form to the IIFC. The User agrees to maintain supporting documentation for criminal intelligence information entered in the Database in a format approved by the IIFC.

Submissions shall not include information about political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity. The User shall not submit any information which has been obtained in violation of any applicable Federal, State, or local law or ordinance.

The IIFC shall collect and maintain criminal intelligence information in the Database concerning an individual or an organization only if there is a reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity. Criminal intelligence information must achieve a reasonable suspicion standard before it is retained in the Database. Reasonable suspicion is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

Further, the provisions of Indiana Code § 5-2-4 *et. al*., reproduced below, must be strictly followed:

Ind. Code § 5-2-4

1. DEFINITIONS

As used in this chapter, unless the context otherwise requires:

(1) "Criminal history information" means information collected by criminal justice agencies or individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release.

(2) "Criminal intelligence information" means information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity, including terrorist activity. "Criminal intelligence information" does not include criminal investigative information, which is information on identifiable individuals compiled in the course of the investigation of specific criminal acts.

(3) "Criminal justice agency" means any agency or department of any level of government which performs as its principal function the apprehension, prosecution,

adjudication, incarceration, or rehabilitation of criminal offenders, or location of parents with child support obligations under 42 U.S.C. 653. The term includes:

(A) a nongovernmental entity that performs as its principal function the:

(i) apprehension, prosecution, adjudication, incarceration, or rehabilitation of criminal offenders; or

(ii) location of parents with child support obligations under 42 U.S.C. 653;

under a contract with an agency or department of any level of government;

(B the department of homeland security; and

(C) the Indiana intelligence fusion center established by IC 10-11-9-2.

2. FILES RESTRICED

Criminal intelligence information shall not be placed in a criminal history file, nor shall a criminal history file indicate or suggest that a criminal intelligence file exists on the individual to whom the information relates. Criminal history information may, however, be included in criminal intelligence files.

3. CRIMINAL ACTIVITY; RELEVANCY; RESTRICTION

Criminal intelligence information concerning a particular individual shall be collected and maintained by a state or local criminal justice agency only if grounds exist connecting the individual with known or suspected criminal activity and if the information is relevant to that activity.

4. RENTENTION; DESTRUCTION

Criminal intelligence information shall be reviewed by the chief executive officer of the criminal justice agency at regular intervals to determine whether the grounds for retaining the information still exist and if not, it shall be destroyed.

5. POLITICAL, RELIGIOUS, OR SOCIAL VIEWS; ASSOCIATAIONS OR ACTIVITES RESTRICTED

No criminal justice agency shall collect or maintain information about the political, religious or social views, associations or activities of any individual, group, association, corporation, limited liability company, business, or partnership unless such information directly relates to an investigation of past or threatened criminal acts or activities and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal acts or activities.

6. CONFIDENTIALITY; AUTHORIZED DISCLOSURE

Criminal intelligence information is hereby declared confidential and may be disseminated only in accordance with section 7 of this chapter, and only if the agency

making the dissemination is satisfied that the need to know and intended uses of the information are reasonable and that the confidentiality of the information will be maintained.

7. UNLAWFUL DISCLOSURE; DISCLOSURE TO CERTAIN PERSONS PERMITTED TO AVOID IMMINENT DANGER TO LIFE OR PROPERTY

(a) Except as provided in subsection (b), a person who knowingly releases criminal intelligence information to an agency or person other than a criminal justice agency commits a Class A misdemeanor.

(b) When necessary to avoid imminent danger to life or property, a criminal justice agency may disseminate an assessment of criminal intelligence information to:
(1) a government official; or
(2) another individual:
(A) whose life or property is in imminent danger;
(B) who is responsible for protecting the life or property of another person; or
(C) who may be in a position to reduce or mitigate the imminent danger to life or property.

Entry of individuals or organizations into the Database shall be made only in circumstances that meet the following standards:

A. ENTRY OF AN INDIVIDUAL INTO THE DATABASE

For entry of an individual into the database, a User must have a reasonable suspicion that the individual means to commit, to attempt to commit, to conspire to commit a violation of, or aiding and abetting in a violation of any criminal activities or is a member of an organization that is involved in criminal conduct or activity.

B. INDIVIDUAL WHO IS A MEMBER OF A GANG OR CRIMINAL ORGANIZATION

In determining if enough evidence exists to create a reasonable suspicion that an individual is a member of or is associated with a gang or a criminal organization for entry into the database, Users shall weigh and consider the following (IC 35-45-9-3):

(1) an admission of criminal organization membership by the person;
(2) a statement by:
(A) a member of the person's family;
(B) the person's guardian; or

(C) a reliable member of the criminal organization; stating the person is a member of a criminal organization;

(3) the person having tattoos identifying the person as a member of a criminal organization;

(4) the person having a style of dress that is particular to members of a criminal organization;

(5) the person associating with one (1) or more members of a criminal organization;

(6) physical evidence indicating the person is a member of a criminal organization;

(7) an observation of the person in the company of a known criminal organization member on at least three (3) occasions;

(8) communications authored by the person indicating criminal organization membership, promotion of the membership in a criminal organization, or responsibility for an offense committed by a criminal organization;

(9) the person's use of the hand signs of a criminal organization; and

(10) the person's involvement in recruiting criminal organization members.

As long as the User can articulate facts that show a reasonable suspicion, any of the above factors, individually or in combination, may justify entry of an individual into the database.

C. ENTRY OF A CRIMINAL ORGANIZATION

For entry of a criminal organization into the database, a user must have a reasonable suspicion that the organization is involved in criminal conduct or activity and that the organization meets the following definition (IC 35-45-9-1):

A "Criminal Organization" is:
A formal or informal group with at least three (3) members that specifically:

(1) either:

(A) promotes, sponsors, or assists in;

(B) participates in; or

(C) has as one (1) of its goals; or

(2) requires as a condition of membership or continued membership;

the commission of a felony, an act that would be a felony if committed by an adult, or a battery offense included in IC 35-42-2.

IX. CRIMINAL INTELLIGENCE INFORMATION DISSEMINATION:

A. IIFC DISSEMINATION OF USER'S CRIMINAL INTELLIGENCE INFORMATION

All information entered into the Database shall be considered open for dissemination by the IIFC to other Users for all lawful purposes unless the submitting User indicates that the dissemination

of a specific entry is restricted. Users will not be able to access restricted entries by querying the Database. However, the IIFC shall retain access to all entries submitted to the Database, including all restricted entries. If the IIFC seeks to disseminated a restricted entry for a lawful purpose, the IIFC shall adhere to blind deconfliction policy seeking permission of the originating agency prior to any dissemination.

B. USER DISSEMINATION OF CRIMINAL INTELLIGENCE INFORMATION

The User agrees that criminal intelligence information may only be used as lead information and shall not include criminal intelligence information in criminal case or incident reports. Using the criminal intelligence information as lead information will require the User to develop probable cause information independent from the criminal intelligence information. Criminal intelligence information shall not be placed in a criminal history file, nor shall a criminal history file indicate or suggest that a criminal intelligence information file exists on the individual to whom the information relates. Criminal history information may, however, be included in criminal intelligence information files.

The User agrees to only disseminate criminal intelligence information in the Database in compliance with 28 CFR Part 23 and IC 5-2-4. A User shall disseminate criminal intelligence information only where there is a need-to-know and right-to-know the information in the performance of a law enforcement activity.

The User agrees to only disseminate criminal intelligence information in the Database upon verification of the recipient's need-to-know and right-to-know the criminal intelligence information. The User agrees that it is the User's responsibility to verify the recipient's need-to-know and right-to-know criminal intelligence information. The User agrees to disseminate criminal intelligence information only as per directions of the originator of the criminal intelligence information and only as per the allowable dissemination criteria indicated in the Database. The User agrees to disseminate criminal intelligence information only as per the Privacy Policy of the IIFC. The User agrees to maintain a record of disseminations and authorizes the IIFC to review these records for inspections and audits in compliance with 28 CFR Part 23 and IC 5-2-4. The User agrees to record the following in its dissemination record:

A. Name of the User disseminating the information;
B. Control number of criminal intelligence information item disseminated;
C. Date of dissemination of the information;
D. Name of the individual and agency to whom criminal intelligence information is disseminated;
E. Reason for the dissemination of criminal intelligence information;
F. Description of criminal intelligence information disseminated;
G. Description of additional dissemination directions given to recipient.

_____
Initials

The User may disseminate an assessment of criminal intelligence information to a government official or another individual to avoid imminent danger to life or property. (See IC 5-2-4-7). The User agrees to immediately notify the IIFC when an assessment of criminal intelligence information is disseminated to any individual in order to avoid an imminent danger to life or property.

The User agrees that all derivative intelligence products will properly reference the criminal intelligence information utilized from the Database and the User agrees that all derivative intelligence products will contain dissemination restrictions at no less than the disseminating restrictions of the criminal intelligence information utilized from the Database. The User agrees to share all derivative intelligence products with the IIFC.

The User agrees to complete the Database dissemination record for any item(s) printed from the Database. The IIFC prohibits the use of "Print Screen" or "Copy/Paste" computer functions that avoids the completion of the Database dissemination record. The User agrees to be responsible for maintaining the required level of security for printed criminal intelligence information to prevent its unauthorized use and disclosure.

X. CRIMINAL INTELLIGENCE INFORMATION DELETION:

The User authorizes the IIFC to permanently delete information from the Database when the criminal intelligence information reaches the end of the IIFC determined retention period. The User agrees that this may be done without notification to the User. The User agrees to cause a review for appropriateness of any derivative intelligence products whenever some of the basis for the derivative intelligence products is criminal intelligence information from the Database that has been deleted due to reaching the end of its retention cycle or has been deleted due to no longer meets Database criteria.

XI. AUDITS:

The Participating Agency and User agree to submit to IIFC routine inspections and audits to determine compliance with the IIFC Privacy Policy, 28 CFR Part 23, and IC 5-2-4. The Participating Agency and User agree to submit verification of any User's need-to-know and right-to-know upon the IIFC's request at any time.

XII. INDIANA'S ACCESS TO PUBLIC RECORDS ACT (APRA), IC 5-14-3-1, et seq.:

The IIFC and Participating Agencies are subject to the APRA and the Indiana Preservation of Public Records Act, IC 5-15-1, et seq. If the Participating Agency receives a request under the APRA for records in the Database or generated from the Database, the Participating Agency shall promptly forward the request to the IIFC for review. The IIFC shall designate in writing to the Participating Agency which of those records, if any, the IIFC considers confidential

information or otherwise excepted from public disclosure under the APRA exceptions set forth in IC 5-14-3-4. The Participating Agency shall promptly review the basis for the IIFC's claims, including claims of confidentiality, and shall not disclose the records subject to the IIFC's claims if the Participating Agency concurs with the IIFC's claims. If the Participating Agency determines that its obligations under the APRA requires such disclosure, the Participating Agency shall promptly notify the IIFC of such determination and will not make such disclosure if the IIFC obtains, prior to the expiration of the applicable time frame to respond to such request, either an opinion from the Indiana Public Access Counselor that such disclosure is not required, or a protective order of other relief from any court of competent jurisdiction preventing such disclosure.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

PARTICIPATING AGENCY CERTIFICATION

The Participating Agency head certifies that Users from Participating Agency that have requested access to the Database have a need-to-know and right-to-know criminal intelligence information. The Participating Agency head agrees to notify the IIFC of all changes of employment status for Users from the Participating Agency that negate the Users' need-to-know and right-to-know criminal intelligence information and to annually verify in writing to the IIFC the need-to-know and right-to-know criminal intelligence information for Users within the Participating Agency. The Participating Agency head agrees to maintain the original signed User Agreement and Appendix C of the IIFC Privacy Policy Receipt of IIFC Privacy Policy by IIFC and Non-IIFC Personnel - for each of its Users during the period each User has access to the Database and for an additional three (3) years from the date of termination of the User's access.

Title: _____

Signature:

Print Name: _____

Date: _____

_____
Initials

USER ACKNOWLEDGEMENT

I acknowledge that I must use the Database for lawful, official use and authorized purposes in accordance with this Agreement. I acknowledge and attest to the fact that the law enforcement agency I work for has signed a current Participating Agency Agreement and is aware of and assents to my entering into of this Agreement. I will ensure that I will comply with all provisions of this Agreement and I give my permission for the IIFC to inspect and audit my activities associated with the Database.

Title: _____

Agency: _____

Signature:

Print Name: _____

Date: _____

_____
Initials